Aislamiento de servidor y dominio mediante IPsec y Directiva de grupo

Apéndice A: Descripción general de los conceptos de la directiva IPsec

Actualizado: febrero 16, aaaa

Este apéndice proporciona una descripción general detallada de los términos, procesos y conceptos de IPsec. Está diseñado para proporcionar el nivel básico de comprensión de IPsec tal como se describe en la Guía de *aislamiento de servidor y dominio mediante IPsec y Directiva de grupo*.

El contenido de este apéndice se publicó originalmente como parte de las notas del producto "Using Microsoft Windows IPsec to Help Secure an Internal Corporate Network Server", disponibles en www.microsoft.com/ipsec y preparadas conjuntamente por Microsoft y Foundstone Strategic Security.

La información adicional de las notas del producto describe el primer modelo para la utilización de IPsec en la protección del acceso de red a servidores Microsoft® Windows® internos que procesan o guardan información confidencial. Aunque esta información adicional no es imprescindible para comprender la Guía de *aislamiento de servidor y dominio mediante IPsec y Directiva de grupo*, constituye información general de gran utilidad.

En esta página

Descargar la solución completa

Aislamiento de servidor y dominio mediante IPsec y Directiva de grupo

En esta guía

Introducción

Cuando se crea una directiva IPsec, se configuran reglas IPsec (que determinan el comportamiento de IPsec) y configuraciones (que son válidas independientemente de las reglas configuradas). Tras configurar una directiva IPsec, ésta debe asignarse a un equipo para que entre en vigor. Aunque pueden existir múltiples directivas IPsec en un equipo, sólo puede asignarse una directiva IPsec a un equipo cada vez.

Una regla IPsec determina qué tipo de tráfico debe examinar IPsec, si se permite o bloquea el tráfico, si se negocia la seguridad y cómo autenticar un principal IPsec, entre otras configuraciones. Al configurar una regla IPsec, se configura una lista de filtros que incluye uno o varios filtros, una acción de filtrado, métodos de autenticación, un tipo de conexión y un modo de encapsulación IPsec (modo de transporte o modo de túnel). Una regla IPsec suele configurarse con un objetivo concreto (por ejemplo “Bloquear todo el tráfico entrante de Internet al puerto TCP 135”).

Los filtros definen el tráfico que se desea inspeccionar, de un modo similar a una regla de servidor de seguridad, con direcciones IP de origen y destino, protocolos y números de puerto, si corresponde. Una acción de filtrado define los requisitos de seguridad para el tráfico de red. Puede configurar una acción de filtrado para permitir, bloquear o negociar la seguridad (negociar IPsec). Si configura una acción de filtrado para negociar la seguridad, también deberá configurar métodos de seguridad de intercambio de claves (y su orden de preferencia), y especificar si se acepta el tráfico entrante inicial no seguro, si se permite la comunicación no segura con equipos no compatibles con IPsec y si se utiliza la confidencialidad directa perfecta (PFS).

La configuración y los métodos de seguridad del intercambio de claves determinan los formatos de protocolo IPsec (encabezado de autenticación, AH, o carga de seguridad encapsulada, ESP), los algoritmos de cifrado y operaciones hash, la vigencia de claves y otras configuraciones necesarias para configurar el modo principal de la asociación de claves de Internet (IKE) y las asociaciones de seguridad IPsec (SA). Una SA es el acuerdo de configuraciones de seguridad asociadas con el material de generación de claves. La SA creada durante la primera fase de negociación de IKE se conoce como la SA en modo principal IKE (o también como asociación de seguridad en modo principal ISAKMP). La SA en modo principal IKE protege la propia negociación IKE. Las SA creadas durante la segunda fase de negociación IKE se conocen como las SA IPsec (o también como las SA en modo rápido IKE porque cada negociación en modo rápido IKE negocia la SA IPsec para cada dirección). Las SA IPsec protegen el tráfico de aplicaciones.

Esta sección proporciona información sobre los siguientes conceptos importantes de la directiva IPsec:

- Proceso de negociación IKE
- Filtros de directiva IPsec
- Métodos de seguridad
- Formatos de protocolo IPsec
- Autenticación IKE
- Orden de preferencia del método de seguridad y el método de autenticación IKE
- Opciones de negociación de la seguridad

Para obtener más información sobre los conceptos de la directiva IPsec, acuda al Centro de ayuda y soporte técnico de Microsoft Windows Server™ 2003.

Principio de la página

Filtros de directiva IPsec

Los filtros son la parte más importante de una directiva IPsec. La seguridad puede no ser adecuada si no se especifican los filtros correctos en las directivas de cliente o servidor, o si las direcciones IP cambian antes de que se actualicen los filtros de la directiva. Los filtros IPsec se insertan en la capa IP de la pila de protocolos de red TCP/IP en el equipo, de forma que puedan examinar (filtrar) todos los paquetes IP entrantes o salientes. A excepción de un breve retraso necesario para negociar una relación de seguridad entre dos equipos, IPsec es transparente para las aplicaciones de usuario final y servicios del sistema operativo. Los filtros se asocian con la acción de filtrado correspondiente mediante la regla de seguridad de una directiva IPsec. Windows IPsec admite el modo de túnel IPsec y el modo de transporte IPsec como opción en la regla. La configuración de reglas en el modo de túnel IPsec es muy distinta de la configuración de reglas en el modo de transporte IPsec.

Las reglas de filtrado asociadas con una directiva IPsec son muy similares a las reglas de los servidores de seguridad. Mediante la interfaz de usuario gráfica (GUI) facilitada por el complemento Directiva de seguridad IP de Microsoft Management Console (MMC) puede configurarse IPsec para permitir o bloquear tipos específicos de tráfico según combinaciones de direcciones de origen y de destino, y protocolos y puertos específicos.

Nota: Windows IPsec no es un servidor de seguridad basado en host completo y no es compatible con características de filtrado dinámicas o de estado, como el seguimiento del bit establecido durante la negociación TCP para controlar la dirección en la que puede fluir la comunicación.

Comprensión del filtrado IPsec

Las listas de filtros son simplemente listas de subredes conocidas y direcciones IP de infraestructura. Es importante entender el modo en que se combinan los filtros que se incluyen en todas las reglas para proporcionar los controles de acceso entrantes y salientes necesarios. En esta sección aparecen los detalles más importantes para entender el modo en que los filtros IPsec afectan al procesamiento de paquetes.

El complemento de MMC Monitor IPsec para Windows Server 2003 facilita información más detallada sobre la consignación de filtros IPsec. Cuando el servicio IPsec procesa un conjunto de reglas de directiva IPsec, los filtros se copian en dos tipos para facilitar el control de las dos fases de la negociación IKE:

1. **Filtros IKE de modo principal**. Estos filtros utilizan sólo la dirección de origen y destino de los filtros definidos en la directiva IPsec para controlar IKE de modo principal. Los filtros específicos de IKE de modo principal tienen cada

uno una directiva asociada de negociación IKE de modo principal que define:

- Los métodos de seguridad de modo principal IKE definidos para la directiva IPsec bajo la configuración de intercambio de claves, como la clave de sesión de protección Diffie Hellman y los algoritmos de cifrado e integridad utilizados para proteger la propia negociación IKE.
- La vigencia de IKE de modo principal y los límites del número de claves de sesión generadas a partir de la misma clave de sesión de protección.
- Métodos de autenticación.

2. **Filtros Modo rápido IKE**. Estos filtros contienen toda la información de filtro referente a direcciones, protocolos y puertos. El modo rápido IKE negocia esta definición de filtro para determinar qué tráfico puede protegerse en un par de asociación de seguridad IPsec. Cada filtro específico tiene una importancia correspondiente y un conjunto de métodos de seguridad que definen:

   - Opciones para encapsulación de AH o ESP en modo de transporte o de túnel.
   - Un listado de algoritmos de cifrado e integridad.
   - Las vigencias de la asociación de seguridad IPsec en kilobytes y segundos.
   - La configuración de seguridad de confidencialidad directa perfecta.

Los filtros específicos para modo rápido IKE son una lista de filtros que se otorgan al controlador IPsec para su aplicación. El controlador IPsec hace coincidir todo el tráfico IP entrante y saliente con estos filtros, en el orden especificado por el de mayor importancia. La sección siguiente del proceso de negociación IKE describe el modo en que IKE negocia y administra las asociaciones de seguridad IPsec utilizando estos controles de directiva.

Los filtros que se definen en la directiva IPsec se consideran filtros "genéricos" porque tendrían que interpretarse por el servicio IPsec cuando se aplique la directiva. El servicio IPsec interpreta todos los filtros genéricos en filtros específicos en el momento en que se aplica la directiva IPsec (o cambio) en el equipo. Los filtros específicos tienen un algoritmo integrado para calcular la importancia, u orden, que también hace referencia a lo específico que es el filtro al seleccionar el tráfico. Un valor de importancia más alto corresponde a un filtro más específico. Todos los filtros específicos se clasifican según su importancia. La importancia del filtro se evalúa en primer lugar para la dirección IP, a continuación para los protocolos y finalmente para los puertos que pueden haberse definido en el filtro. Esta estrategia garantiza que el orden de las reglas de una directiva y la consignación de los filtros en cada lista de filtros diferente no tienen ningún efecto sobre el comportamiento de filtrado que impone el controlador IPsec durante el procesamiento de paquetes. Los paquetes se hacen coincidir en primer lugar con los filtros más específicos para reducir el tiempo necesario de procesamiento de cada paquete en relación con el conjunto total de filtros. La acción de filtrado que corresponde al filtro más específico que coincide con un paquete es la única acción que tiene lugar para dicho paquete. El filtro más genérico que puede definirse sería aquel que coincidiera con todas las direcciones IP, todos los protocolos y todos los puertos. Por ejemplo, tenga en cuenta las cuatro definiciones de filtro siguientes:

- Cualquiera <-> Cualquiera, cualquier protocolo
- Cualquiera <-> 192.168.1.0/24, cualquier protocolo
- Cualquiera <-> 192.168.1.10/24, cualquier protocolo
- Cualquiera <-> 192.168.1.10/24, puerto de origen TCP Cualquiera, puerto de destino 25

El filtro Cualquiera a Cualquiera es el filtro más general que puede definirse. Sólo es compatible con Windows Server 2003 y Windows XP Service Pack 2 (SP2). Normalmente, este filtro se utiliza con una acción de bloqueo para conseguir el comportamiento predeterminado de "Denegar todo". Si se utiliza este filtro para bloquear todo el tráfico, el resto de los filtros más específicos podrían considerarse excepciones del primer filtro. Para Windows 2000, el filtro compatible más general es Cualquiera <-> subred, cualquier protocolo, o bien Cualquiera <-> Mi dirección IP si no se utilizan subredes.

Los cuatro filtros coincidirían con el tráfico entrante de cualquier dirección IP a 192.168.1.10, utilizando el puerto TCP 25 y las respuestas salientes correspondientes del puerto 25. El cuarto filtro es el más específico porque define una dirección IP de destino, un protocolo y un número de puerto. Si el controlador IPsec impone los cuatro filtros, un paquete entrante destinado al puerto TCP 25 sólo coincidiría con el cuarto filtro, el más específico. Si un sistema remoto enviara tráfico TCP a un puerto distinto al 25 para 192.168.1.10, coincidiría con el tercer filtro. Finalmente, si se enviara tráfico a cualquier dirección IP de la subred 192.168.1.0 a excepción de 192.168.1.10, el segundo filtro sería el más específico para dicho

tráfico.

Problemas potenciales en el diseño de filtros

Existen algunas opciones referentes a la combinación de direcciones de origen y de destino que no deben utilizarse en la definición de filtros. Tal como mencionamos anteriormente, los filtros que especifican Cualquier dirección IP a Cualquier dirección IP deben evitarse para los hosts con Windows 2000.

Normalmente, cuantos más filtros incluya una directiva, mayor será el impacto sobre el rendimiento del procesamiento de paquetes. Este impacto se manifiesta en forma de rendimiento reducido, así como en una mayor utilización de la CPU y de la memoria del núcleo de bloque no paginado. Resulta muy difícil estimar cuál es el impacto preciso sobre el rendimiento porque depende del volumen total de tráfico, la cantidad de tráfico protegido por IPsec que se procesa y la carga de la CPU del equipo. Por lo tanto, en la planificación deberá incluirse la evaluación del rendimiento de los diseños de directivas IPsec. El impacto de unos cuantos centenares de filtros seguramente sólo será perceptible en los equipos de muy alto rendimiento.

Windows 2000 no incluye optimizaciones para la administración de números elevados de filtros. El controlador IPsec debe explorar toda la lista de filtros secuencialmente para encontrar una coincidencia.

En Windows XP y Windows Server 2003 se incorporaron muchas optimizaciones para acelerar el procesamiento de filtros de forma que fuera posible utilizar un mayor número de filtros en la directiva IPsec. Se optimizaron los filtros con el formato "De <dirección IP> a <dirección IP>", independientemente de protocolo o puertos, con la utilización del controlador Clasificador de paquetes genéricos (GPC) para conseguir búsquedas extremadamente rápidas. El controlador GPC puede administrar prácticamente cualquier número de estos filtros sin que se vea afectado el rendimiento. Por lo tanto, las listas extensas de exenciones con el formato "Mi dirección IP a <dirección IP exenta específica>" no presentan ningún problema, siempre y cuando haya suficiente memoria del núcleo no paginado disponible para incluir toda la lista de filtros. Los filtros que no tienen una dirección IP específica de origen y de destino no pueden optimizarse mediante el controlador GPC y, por lo tanto, los filtros del tipo "Cualquier IP <-> IP (o subred) específica" requieren una búsqueda secuencial. La implementación se mejora con Windows 2000.

El uso de Mi dirección IP podría ser apropiado en muchos casos, pero también puede provocar problemas en aquellos hosts con muchas direcciones IP, como un servidor Web que aloja muchos sitios Web virtuales. También puede provocar un retraso en la disponibilidad del filtrado de paquetes del controlador IPsec si hay muchos filtros que utilizan Mi dirección IP. El servicio IPsec los procesa durante el inicio del servicio y siempre que se produce un cambio de dirección. El retraso puede provocar una ventana de vulnerabilidad o retrasos en la conexión segura con IPsec. De nuevo, un análisis del rendimiento deberá confirmar el impacto sobre un diseño de directiva concreto.

Mi dirección IP quizás sea más apropiado cuando se permite o deniega el tráfico a un puerto o protocolo específico. Por ejemplo, en el diseño de la directiva IPsec para Woodgrove Bank, los filtros "Mi dirección IP" se utilizan para crear un filtro más específico que permita que el tráfico del Protocolo de mensajes de control de Internet (ICMP) se envíe y reciba en texto sin cifrar entre todos los equipos.

Si a un cliente móvil de la organización se le asigna una regla "Mi dirección IP <-> Cualquier dirección IP" y, a continuación, se ubica en una red externa, quizás el cliente móvil no pueda comunicarse en dicho entorno. Si se permite al cliente el Retroceso a texto no cifrado, el cliente experimentará retrasos de tres segundos y superiores cuando se conecte a cada destino. Si el destino responde con una respuesta IKE, la negociación IKE dará error, ya que IKE no podrá llevar a cabo la autenticación utilizando la confianza de dominio (Kerberos). Claramente, si se utilizan direcciones privadas RFC 1918 como subredes de red interna, los clientes móviles se verán afectados cuando se conecten en hoteles, redes domésticas e incluso otras redes internas. Si los clientes móviles experimentan problemas de conectividad, quizás necesiten derechos de Administrador local para detener el servicio IPsec cuando se conecten a otras redes. Por ello puede ser necesario utilizar un comando de inicio de sesión de dominio para comprobar si el servicio IPsec se está ejecutando cuando se conectan a la red interna.

Windows 2000 no se diseñó originariamente para el filtrado de paquetes utilizando direcciones de difusión y multidifusión porque no era posible proteger este tráfico con la negociación IKE. Por lo tanto, los tipos de paquete de difusión y multidifusión formaban parte de las exenciones predeterminadas originales que omitían los filtros IPsec. Consulte el artículo 811832 de Microsoft Knowledge Base (KB) "IPsec Default Exemptions Can Be Used to Bypass IPsec Protection in Some Scenarios" (Las exenciones predeterminadas de IPsec pueden utilizarse para omitir la protección IPsec en algunos escenarios), disponible en http://support.microsoft.com/kb/811832, donde encontrará una explicación detallada de las implicaciones para la seguridad de las exenciones predeterminadas y los cambios implementados en el Service Pack 3 para eliminar algunas de ellas por defecto. La integración de TCP/IP con IPsec en Windows XP y Windows Server 2003 se mejoró para filtrar todo tipo de paquetes IP. Sin embargo, puesto que IKE no puede negociar la seguridad para difusión y multidifusión, la compatibilidad con el filtrado es limitada. Consulte el artículo 810207 de KB, "IPsec default exemptions are

removed in Windows Server 2003" (Se eliminan las exenciones predeterminadas IPsec en Windows Server 2003), disponible en http://support.microsoft.com/kb/810207, para obtener más información sobre la supresión de las exenciones predeterminadas y el grado de compatibilidad de filtrado para el tráfico de difusión y multidifusión. Windows XP SP2 admite las mismas capacidades de filtrado Cualquiera <-> Cualquiera que Windows Server 2003.

Principio de la página

Proceso de negociación IKE

El protocolo IKE está diseñado para establecer, de forma segura, una relación de confianza entre cada equipo, negociar opciones de seguridad y producir dinámicamente material criptográfico de generación de claves secretas compartido. Para garantizar una comunicación satisfactoria y segura, IKE lleva a cabo una operación de dos fases: negociación de fase 1 (modo principal) y negociación de fase 2 (modo rápido). Durante cada fase puede garantizarse la confidencialidad y la autenticación mediante el uso de algoritmos de cifrado y autenticación acordados entre los dos equipos durante las negociaciones de seguridad.

Negociación de modo principal

Durante la negociación de modo principal, los dos equipos establecen un canal seguro y autenticado. En primer lugar se negocian los siguientes parámetros de directiva IPsec: el algoritmo de cifrado (DES o 3DES), el algoritmo de integridad (MD5 o SHA1), el grupo Diffie-Hellman que se utilizará para el material base de generación de claves (Grupo 1, Grupo 2 o, en Windows Server 2003, Grupo 2048) y el método de autenticación (protocolo Kerberos versión 5, certificado de clave pública o clave previamente compartida). Tras la negociación de los parámetros de la directiva IPsec, se completa el intercambio Diffie-Hellman de valores públicos. El algoritmo Diffie-Hellman se utiliza para generar claves secretas, compartidas y simétricas entre equipos. Tras completar el intercambio Diffie-Hellman, el servicio IKE de cada equipo genera la clave de sesión de protección que se utiliza para proteger la autenticación. La clave de sesión de protección se utiliza, junto con los métodos y algoritmos de negociación, para la autenticación de identidades. El iniciador de la comunicación presenta entonces una oferta de una asociación de seguridad potencial al contestador. El contestador puede enviar una respuesta en la que acepte la oferta o bien una respuesta con alternativas. El resultado de una negociación de modo principal IKE es una SA de modo principal.

Negociación de modo rápido

Durante la negociación de modo rápido, se establece un par de SA IPsec para contribuir a la protección del tráfico de la aplicación, que puede incluir los paquetes que se envían por TCP, el protocolo de datagrama de usuario (UDP) y otros protocolos. En primer lugar se negocian los siguientes parámetros de directiva: el formato del protocolo IPsec (AH o ESP), el algoritmo hash para la integridad y autenticación (MD5 o SHA1) y el algoritmo para el cifrado (DES o 3DES), cuando corresponda. Durante ese período se alcanza un acuerdo común en cuanto al tipo de paquetes IP que se transportarán en el par SA IPsec que se establece. Tras negociar los parámetros de la directiva IPsec, se actualiza o intercambia el material de la clave de sesión (claves criptográficas y vigencia de las claves, en segundos y kilobits, para cada algoritmo).

Cada SA IPsec se identifica mediante un índice de parámetro de seguridad (SPI), que se inserta en el encabezado IPsec de cada paquete enviado. Un SPI identifica la SA IPsec entrante y el otro la SA IPsec saliente.

SA de modo principal IKE y SA IPsec

Cada vez que se utiliza IPsec para contribuir en la protección del tráfico, se establecen una SA de modo principal IKE y dos SA IPsec. En el escenario de ejemplo, para que tengan lugar comunicaciones protegidas por IPsec entre CORPCLI y CORPSRV, se establecen las SA siguientes:

CORPCLI [IP1] **<--------** SA de modo principal IKE [IP1, IP2] **----->** [IP2] CORPSRV

CORPCLI [IP1] **----------** SA IPsec [SPI=x] **----------->** [IP2] CORPSRV

CORPCLI [IP1] **<--------** SA IPsec [SPI=y] **----------** [IP2] CORPSRV

donde:

- IP1 es la dirección IP de CORPCLI.
- IP2 es la dirección IP de CORPSRV.
- x es el SPI que identifica la SA IPsec entrante para CORPSRV desde CORPCLI.
- y es el SPI que identifica la SA IPsec saliente para CORPSRV desde CORPCLI.

Tal como indica este resumen, la SA de modo principal IKE entre CORPCLI y CORPSRV es bidireccional. Cualquier equipo puede iniciar una negociación de modo rápido utilizando la protección que facilita la SA de modo principal IKE. Las SA IPsec no dependen del estado de protocolos de capa superior. Por ejemplo, pueden establecerse y finalizarse conexiones TCP mientras continúan las SA IPsec y las SA IPsec pueden caducar antes de que finalice una conexión TCP. IKE intenta la renegociación para evitar que se interrumpa una conexión utilizando la negociación de modo rápido para establecer dos pares de SA IPsec nuevos, antes de que caduque la vigencia del par de SA IPsec existente. Aunque este proceso normalmente se conoce como "cambio de claves de la asociación de seguridad IPsec", en realidad se establecen dos SA IPsec nuevas. El ciclo de vida de la SA de modo principal IKE se mide sólo por el tiempo y el número de SA IPsec que se han intentado (no por el número de bytes de datos que se transfieren en el protocolo IKE). La SA de modo principal IKE caduca independientemente del par SA IPsec. Si se necesita un par SA IPsec nuevo, se renegocia automáticamente una SA de modo principal IKE de la forma adecuada (cuando ha caducado una SA de modo principal). Según el diseño de IETF (Internet Engineering Task Force), IKE debe ser capaz de cambiar las claves de la SA de modo principal y negociar en el modo rápido IKE en cualquier dirección. Por lo tanto, el método de autenticación que se configura en la directiva IPsec de ambos equipos para la SA de modo principal IKE debe permitir la autenticación en la dirección desde la que se inicia la negociación de modo principal IKE. Del mismo modo, la configuración de la directiva IPsec en la acción de filtrado para modo rápido debe permitir la negociación bidireccional de modo rápido.

Principio de la página

Métodos de seguridad

Los métodos de seguridad se utilizan durante la negociación de modo principal IKE para definir los algoritmos de cifrado y hash y el grupo Diffie-Hellman que se utiliza para crear la SA de modo principal y para contribuir en la protección del canal de negociación IKE. También se utilizan métodos de seguridad durante la negociación de modo rápido para definir el modo de encapsulación (de transporte o túnel), el formato del protocolo IPsec (AH o ESP), los algoritmos de cifrado y hash y las vigencias de clave que se utilizan para crear las SA entrantes y salientes de modo rápido.

Principio de la página

Modos de encapsulación IPsec y formatos de protocolo

IPsec ayuda a proteger los datos de un paquete IP mediante la protección cifrada de una carga IP. La protección facilitada depende del modo en que se utiliza IPsec y del formato de protocolo. IPsec puede utilizarse en modo de transporte o en modo de túnel.

Modos de encapsulación IPsec

El modo de túnel IPsec normalmente se utiliza para proteger el tráfico de sitio a sitio (también se conoce como de puerta de enlace a puerta de enlace o de enrutador a enrutador) entre redes, como la conexión en red entre sitios a través de Internet. Si se utiliza el modo de túnel IPsec, la puerta de enlace de envío encapsula todo el paquete IP original creando un nuevo paquete IP que seguidamente se protege mediante uno de los formatos de protocolo IPsec (AH o ESP). Para obtener más información acerca de IPsec en modo de túnel, consulte el capítulo “Deploying IPsec” de *Deploying Network Services*, en el Windows Server 2003 Deployment Kit, disponible en la dirección http://go.microsoft.com/fwlink/?LinkId=8195.

El modo de transporte IPsec se utiliza para proteger las comunicaciones de host a host y es el modo predeterminado para Windows IPsec. Si se utiliza IPsec en modo de transporte, IPsec cifra sólo la carga IP, y no el encabezado IP. Windows IPsec se utiliza en modo de transporte principalmente para proteger la comunicación de extremo a extremo, por ejemplo entre clientes y servidores.

Formatos de protocolo IPsec

IPsec admite dos formatos de protocolo: AH o ESP. El modo de transporte IPsec encapsula la carga IP original con un encabezado IPsec (AH o ESP).

AH

AH proporciona autenticación de origen de datos, integridad de datos y protección antieco para todo el paquete (tanto el encabezado IP, como la carga de datos que transporta el paquete), excepto los campos del encabezado IP que pueden cambiar en tránsito. AH no proporciona confidencialidad de datos, es decir, no cifra los datos. Los datos pueden leerse pero están protegidos contra modificaciones e imitaciones. Tal como muestra la figura siguiente, se proporciona integridad y autenticación mediante la ubicación del encabezado AH entre el encabezado IP y los datos TCP.

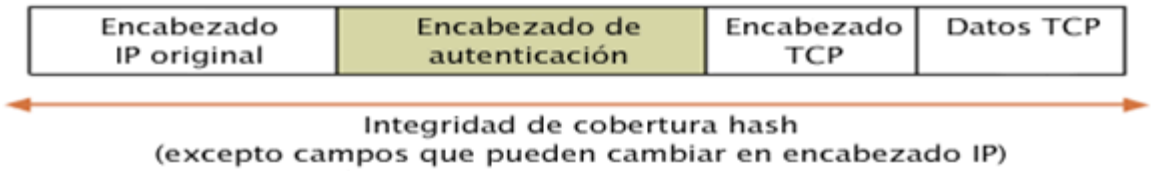

Figura A.1 Encabezado de autenticación en un paquete
Ver imagen a tamaño completo

Para utilizar AH, en el cuadro de diálogo **Configuración de método de seguridad personalizado** de las propiedades de la regla pertinente, seleccione la casilla de verificación **Integridad de direcciones y datos sin cifrado (AH)** y, a continuación, especifique el algoritmo de integridad que desea utilizar.

ESP

ESP proporciona autenticación de origen de datos, integridad de datos, protección antieco y la opción de confidencialidad sólo para la carga IP. ESP en modo de transporte no protege todo el paquete con una suma de comprobación de cifrado. El encabezado IP no está protegido. Tal como se muestra en la figura siguiente, el encabezado ESP se coloca antes de los datos TCP, y la parte final de ESP y la parte final de autenticación ESP se colocan después de los datos TCP.

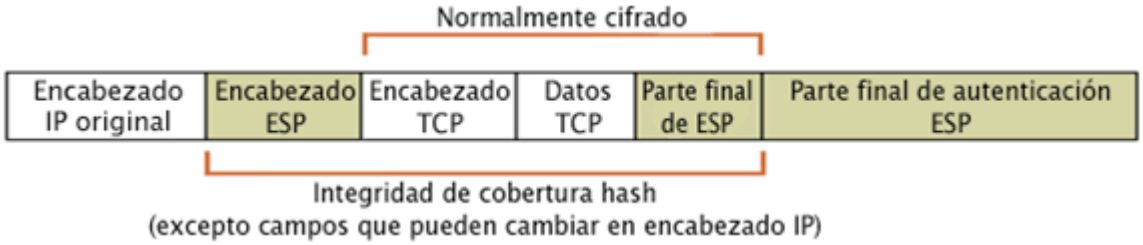

Figura A.2 Datos ESP en un paquete
Ver imagen a tamaño completo

Para utilizar ESP, en el cuadro de diálogo **Configuración de método de seguridad personalizado** de las propiedades de la regla pertinente, seleccione la casilla de verificación **Integridad de direcciones y cifrado (ESP)** y, a continuación, especifique los algoritmos de integridad y cifrado que desea utilizar.

Principio de la página

Autenticación IKE

IKE utiliza la autenticación mutua entre equipos para establecer comunicaciones de confianza y requiere el uso de uno de los siguientes métodos de autenticación: protocolo Kerberos versión 5, un certificado de infraestructura de claves públicas (PKI) X.509 versión 3 para equipos o una clave previamente compartida. Los dos extremos de comunicación deben tener como mínimo un método de autenticación común; de lo contrario, la comunicación dará error.

Proceso de autenticación IKE

Durante la negociación IKE, el iniciador IKE propone una lista de métodos de autenticación al contestador IKE. El contestador utiliza la dirección IP de origen del iniciador para identificar qué filtro controla la negociación IKE. La lista de métodos de autenticación que corresponde al filtro en la directiva IPsec del contestador se utiliza para seleccionar un método de autenticación de la lista del iniciador. El contestador responde para informar al iniciador del método de autenticación acordado. Si el método de autenticación seleccionado falla, IKE no proporciona un método para probar un método de autenticación distinto. Si la autenticación es satisfactoria y la negociación de modo principal se completa satisfactoriamente, la SA de modo principal dura un período de ocho horas. Si todavía se están transmitiendo datos cuando finaliza este período de ocho horas, la SA de modo principal se renegocia automáticamente.

Métodos de autenticación IKE

Es importante seleccionar el método de autenticación apropiado para la directiva IPsec. Una regla de directiva IPsec asocia cada dirección IP de un filtro con una lista de métodos de autenticación, de forma que IKE pueda determinar qué lista de métodos de autenticación utilizar con cada dirección IP.

El protocolo de autenticación Kerberos, versión 5

El protocolo Kerberos versión 5 es el estándar de autenticación predeterminado en los dominios de Active Directory de Windows 2000 y Windows Server 2003. Cualquier equipo del dominio o de un dominio de confianza puede utilizar este método de autenticación.

Si se utiliza la autenticación Kerberos , durante la negociación de modo principal, cada principal IPsec envía la identidad del equipo sin cifrar al otro principal. La identidad del equipo no se cifra hasta que tiene lugar el cifrado de toda la carga de identidad durante la fase de autenticación de la negociación de modo principal. Un atacante puede enviar un paquete IKE que provoque que el principal IPsec que responde exponga su identidad de equipo y pertenencia a dominio. Por ello se recomienda la autenticación basada en certificados para proteger los equipos conectados a Internet.

De forma predeterminada, en Windows 2000 hasta Service Pack 3 y en Windows XP, el tráfico del protocolo Kerberos queda exento del filtrado IPsec. Para corregir la exención del tráfico de protocolo Kerberos, es preciso modificar el registro y agregar un filtro IPsec apropiado para proteger este tráfico. Para obtener más información acerca de las exenciones predeterminadas en Windows 2000 y Windows Server 2003, consulte el documento Special IPsec considerations - Creating, modifying, and assigning IPsec policies, disponible en el sitio Web de Microsoft: www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/sag_IPSECbpSpecial.asp.

Autenticación basada en certificados de clave pública

En Windows 2000 Server, puede utilizar los servicios de Certificate Server para administrar automáticamente certificados de equipo para IPsec a lo largo del ciclo de vida del certificado. Los servicios de Certificate Server se integran con Active Directory y la Directiva de grupo, y simplifican la implementación de certificados permitiendo la inscripción automática y la renovación de certificados, y proporcionando varias plantillas de certificados predeterminadas compatibles con IPsec. Para utilizar certificados en la autenticación IKE, se definirá una lista ordenada de entidades emisoras de certificados raíz (CA) aceptables que pueden utilizarse, en lugar de qué certificado en concreto debe utilizarse. Ambos equipos deben tener una entidad emisora de certificados raíz común en su directiva IPsec, y los clientes deben tener un certificado de equipo asociado.

Durante el proceso de selección de certificados, IKE lleva a cabo una serie de comprobaciones para asegurarse de que se satisfacen determinados requisitos para el certificado del equipo. Por ejemplo, el certificado del equipo debe tener una longitud de clave pública superior a 512 bits y emplear un uso de claves de firma digital.

Nota: los certificados obtenidos del servicio de Certificate Server con las opciones avanzadas establecidas para **Habilitar la protección segura de claves privadas** no funcionan para la autenticación IKE porque no es posible especificar el número de identificación personal (PIN) necesario para acceder a la clave privada de un certificado de equipo durante la negociación IKE.

Claves previamente compartidas

Si no está utilizando la autenticación Kerberos y no tiene acceso a una CA, puede utilizar una clave previamente compartida. Por ejemplo, un equipo independiente de la red puede necesitar utilizar una clave previamente compartida porque ni la autenticación Kerberos (a través de la cuenta de dominio del equipo) ni los certificados de una CA permiten una autenticación IKE satisfactoria en algunos escenarios.

Importante: las claves previamente compartidas son fáciles de implementar pero pueden quedar expuestas si no se utilizan correctamente. Microsoft no recomienda el uso de la autenticación mediante claves previamente compartidas en Active Directory porque el valor de la clave no se guarda de forma segura y, por lo tanto, es difícil mantenerlo en secreto. El valor de la clave previamente compartida se guarda en texto sin formato en una directiva IPsec. Cualquier miembro del grupo de administradores locales puede ver una directiva IPsec local, y cualquier servicio del sistema con derechos de usuario de sistema local puede leer una directiva IPsec local. De forma predeterminada, cualquier usuario autenticado en el dominio puede ver una clave previamente compartida si se guarda en una directiva IPsec basada en Active Directory. Además, si un atacante lograra capturar paquetes de negociación IKE, existen métodos publicados que le permitirán descubrir los valores de la clave previamente compartida.
Para obtener más información, consulte "Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets", disponible en http://go.microsoft.com/fwlink/?LinkId=18769.

La autenticación mediante claves previamente compartidas se facilita para garantizar la interoperabilidad y la compatibilidad de los estándares de RFC. Si necesita utilizar la autenticación mediante claves previamente compartidas, utilice un valor de clave aleatorio de 25 caracteres como mínimo y una clave previamente compartida distinta para cada par de direcciones IP. De esta forma conseguirá reglas de seguridad diferentes para cada destino y una clave previamente

compartida en peligro sólo afectará a los equipos que compartan dicha clave.

Comprobación de CRL IPsec

Si emplea la autenticación basada en certificados, también puede habilitar la comprobación de listas de revocación de certificados (CRL) IPsec. De forma predeterminada, en Windows 2000 no se comprueban automáticamente las CRL IPsec durante la autenticación de certificados IKE.

Para habilitar la comprobación de CRL IPsec

Precaución: la edición incorrecta del registro puede dañar el sistema gravemente. Antes de hacer cambios en el Registro, debe hacer copias de seguridad de todos los datos del equipo.

1. En **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent**, agregue una clave Oakley nueva, con la entrada DWORD StrongCrlCheck.
2. Asigne a esta entrada cualquier valor entre 0 y 2, donde:
   - Con el valor **0** se deshabilita la comprobación de CRL (predeterminado en Windows 2000).
   - Con el valor **1** se intenta la comprobación de CRL y la validación de certificado fracasa sólo si se revoca el certificado (predeterminado en Windows XP y Windows Server 2003). El resto de errores que puedan surgir durante la comprobación de CRL (por ejemplo, que no pueda tenerse acceso a la URL de revocación) no provocan errores en la validación de certificados.
   - El valor **2** habilita la comprobación de CRL segura, es decir, la comprobación de CRL es obligatoria y la validación del certificado falla si surge cualquier error durante el procesamiento de la CRL. Establezca este valor de registro para una seguridad mejorada.
3. Siga uno de estos pasos:
   - Reinicie el equipo.
   - Detenga y vuelva a iniciar el servicio IPsec ejecutando los comandos **net stop policyagent** y **net start policyagent** en el símbolo del sistema.

     Nota: la comprobación de CRL IPsec no garantiza que la validación de certificados falle inmediatamente cuando se revoca un certificado. Existe un retraso entre el momento en que el certificado revocado se incluye en una CRL actualizada y publicada y el momento en que el equipo que se encarga de la comprobación de CRL IPsec recupera esta CRL. El equipo no recupera una CRL nueva hasta que caduca la CRL actual o hasta la próxima vez que se publica la CRL. Las CRL se almacenan en la memoria caché y en \Documents and Settings*NombreUsuario*\Configuración local\Archivos temporales de Internet mediante CryptoAPI. Puesto que las CRL permanecen aunque se reinicie el equipo, si surge un problema de caché de CRL, reiniciar el equipo no resolverá dicho problema.

Principio de la página

Orden de preferencia de los métodos de autenticación IKE y el método de seguridad

Puede configurarse una regla IPsec para especificar sólo un método de autenticación o un método de seguridad. También es posible especificar una lista de métodos de autenticación y seguridad preferidos. El orden de preferencia se aplica a los métodos de autenticación y a los métodos de seguridad, de forma que puede especificar cada método de mayor a menor preferencia. Por ejemplo, puede especificar que se ofrezcan como métodos de autenticación tanto el protocolo Kerberos versión 5 como la autenticación mediante certificados de clave pública, pero asignar al protocolo Kerberos una mayor preferencia, tal como muestra la figura siguiente.

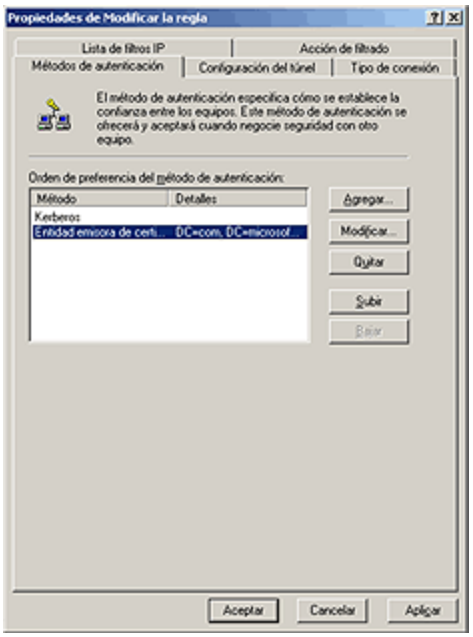

Figura A.3 Orden de preferencia del método de autenticación

Si un cliente intenta conectarse a CORPSRV pero sólo acepta certificados de clave pública para la autenticación, CORPSRV utilizará este método de autenticación y seguirá estableciendo una comunicación. IKE debe poder utilizar satisfactoriamente el método de autenticación seleccionado; de lo contrario, se bloqueará la comunicación. IKE no intentará utilizar un método de autenticación distinto si la negociación da error. El mismo principio es válido para los métodos de seguridad donde, por ejemplo, ESP tiene mayor preferencia que AH.

Principio de la página

Opciones de negociación de seguridad

Es posible configurar si una directiva IPsec permite el retroceso a texto no cifrado (retroceso a comunicación no segura), el paso de sucesos entrante y la PFS de clave de sesión en la ficha **Métodos de seguridad** de las propiedades de una acción de filtrado. Puede configurar las PFS de clave de sesión de protección en el cuadro de diálogo **Valores de intercambio de claves** de las propiedades generales de una regla.

Retroceso a texto no cifrado

Si se permite el retroceso a texto no cifrado, el tráfico se protege mediante IPsec cuando es posible (si el equipo en el otro extremo de la conexión admite IPsec con una acción de filtrado y un filtro complementarios en su directiva), pero el tráfico puede enviarse sin proteger si el principal no tiene una directiva IPsec para responder a la petición de negociación de seguridad. Si el principal no responde a la petición de negociación de seguridad en tres segundos, se crea una SA para tráfico en texto sin formato (una SA por software). Las SA por software permiten la comunicación normal TCP/IP sin que tenga lugar una encapsulación IPsec. Tenga en cuenta que aunque IPsec podría no proteger dicho tráfico (por ejemplo, el tráfico podría protegerse mediante el cifrado de Protocolo ligero de acceso a directorios, LDAP, o los mecanismos de autenticación de llamada a procedimiento remoto, RPC). Si el principal no responde en tres segundos y la negociación de seguridad da error, se bloquea la comunicación que coincide con el filtro correspondiente.

Retroceso a texto no cifrado es un parámetro que permite la interoperabilidad con:

- Equipos con sistemas operativos anteriores a Windows 2000
- Equipos con Windows 2000 o sistemas posteriores que no tienen la directiva IPsec configurada
- Equipos con sistemas operativos que no son de Microsoft y no son compatibles con IPsec

Para habilitar o deshabilitar el retroceso a texto no cifrado, en la ficha **Métodos de seguridad** de las propiedades de una acción de filtrado, active o desactive la casilla de verificación **Permitir comunicación no segura con equipos ajenos a IPsec**.

Puede habilitar o deshabilitar esta opción para cada directiva de cliente. Si habilita esta opción y el servidor no responde a

la petición del cliente de negociar la seguridad, puede permitir que el cliente efectúe un retroceso a texto no cifrado. Si desactiva esta casilla de verificación y el servidor no responde a la petición del cliente de negociar la seguridad, la comunicación se bloquea. En algunos casos, resulta útil permitir el retroceso a texto no cifrado. Sin embargo, IKE sólo permite el retroceso a texto no cifrado sólo si no hay respuesta. Por cuestiones de seguridad, Windows IPsec no permite la comunicación no segura si la negociación IKE da error o si surge algún error durante una negociación IKE (tras la respuesta), por ejemplo la imposibilidad de comunicarse o de alcanzar un acuerdo sobre los parámetros de seguridad.

Para implementaciones iniciales, se recomienda seleccionar esta casilla de verificación de modo que el cliente pueda efectuar un retroceso a texto no cifrado y pueda establecerse conectividad inicial cuando IPsec está deshabilitado en el servidor.

Paso de sucesos entrante

Si se permite el paso de sucesos entrante, el tráfico TCP/IP normal entrante (el tráfico no protegido mediante IPsec, por ejemplo, un paquete SYN de TCP) se acepta si coincide con el filtro entrante asociado con la acción de filtrado. El paquete de respuesta del protocolo de capa superior (por ejemplo, un paquete ACK SYN de TCP) coincide con el correspondiente filtro saliente y desencadena una negociación de seguridad. A continuación se negocian dos SA IPsec y el tráfico se protege por IPsec en ambas direcciones. La opción de paso de sucesos entrante permite a un servidor utilizar la regla de respuesta predeterminada para iniciar la negociación de seguridad con los clientes. Si se habilita la regla de respuesta predeterminada en la directiva IPsec de cliente, no será necesario que los clientes mantengan un filtro que contenga la dirección IP del servidor. Si no se habilita la regla de respuesta predeterminada en la directiva IPsec de cliente, no es necesario habilitar la opción de paso de sucesos entrante en la directiva IPsec del servidor. Además, no debe habilitar nunca esta opción en equipos conectados a Internet.

Para habilitar o deshabilitar el paso de sucesos entrante, en la ficha **Métodos de seguridad** de las propiedades de una acción de filtrado, active o desactive la casilla de verificación **Permitir comunicación no segura pero responder siempre utilizando IPsec**.

Confidencialidad directa perfecta (PFS) para clave de sesión y clave de sesión de protección

PFS es un mecanismo que determina si el material existente de generación de claves para una clave de sesión de protección puede utilizarse para derivar una clave de sesión nueva. PFS garantiza que el ataque a una sola clave permita el acceso únicamente a los datos protegidos por PFS y no necesariamente a toda la comunicación. Para ello, PFS garantiza que una clave utilizada para proteger una transmisión no puede utilizarse para generar claves adicionales. La PFS de clave de sesión puede utilizarse sin una nueva autenticación y consume menos recursos que la PFS de clave de sesión de protección. Cuando se habilita la PFS de clave de sesión, se lleva a cabo un nuevo intercambio de claves Diffie-Hellman para generar información de generación de claves de sesión de protección.

Si habilita la PFS de clave de sesión en una directiva de servidor, también deberá habilitarla en la directiva de cliente. Puede habilitar las PFS de clave de sesión seleccionando la casilla de verificación **Utilizar confidencialidad directa perfecta (PFS) para clave de sesión**, en el cuadro de diálogo **Valores de intercambio de claves** de las propiedades generales de una regla. La PFS de clave de sesión de protección requiere autenticación y consume gran cantidad de recursos. Requiere una nueva negociación de modo principal para cada negociación de modo rápido que tiene lugar. Puede configurar la PFS de clave de sesión de protección seleccionando la casilla de verificación **Confidencialidad directa perfecta de clave de sesión (PFS)**. Si habilita la PFS de clave de sesión de protección en una directiva de servidor, no será necesario habilitarla en la directiva de cliente. Puesto que habilitar esta opción supone una carga importante, se recomienda habilitar la PFS de clave de sesión o la PFS de clave de sesión de protección *sólo* en entornos hostiles en los que el tráfico IPsec puede estar expuesto a atacantes sofisticados que intentarán poner en peligro la protección de cifrado seguro proporcionada por IPsec.

Principio de la página

Administre su perfil